INTERNAL REVENUE SERVICE
IRS News Release

Media Relations Office | Washington, D.C. | Media Contact: 202.622.4000
www.IRS.gov/newsroom | Public Contact: 800.829.1040

IRS Alerts Public to New Identity Theft Scams

IR-2009-71, August 4, 2009

WASHINGTON —The Internal Revenue Service reminds consumers to avoid identity theft scams that use the IRS name, logo or Web site in an attempt to convince taxpayers that the scam is a genuine communication from the IRS. Scammers may use other federal agency names, such as the U.S. Department of the Treasury.

In an identity theft scam, a fraudster, often posing as a trusted government, financial or business institution or official, tries to trick a victim into revealing personal and financial information, such as credit card numbers and passwords, bank account numbers and passwords, Social Security numbers and more. Generally, identity thieves use someone's personal data to steal his or her financial accounts, run up charges on the victim's existing credit cards, apply for new loans, credit cards, services or benefits in the victim's name and even file fraudulent tax returns.

The scams may take place through e-mail, fax or phone. When they take place via e-mail, they are called "phishing" scams.

The IRS does not discuss tax account matters with taxpayers by e-mail.

The IRS urges consumers to avoid falling for the following recent schemes:

Making Work Pay Refund

This phishing e-mail, which claims to come from the IRS, references the president and the Making Work Pay provision of the 2009 economic recovery law. It says that there is a refundable credit available to workers, consumers and retirees that can be paid into the recipient's bank account if the recipient registers their account information with the IRS. The e-mail contains links to register the account and to claim the tax refund.

In reality, most taxpayers receive their Making Work Pay tax credit, which was designed for wage earners, in their paychecks as a result of decreased tax withholding, not as a lump sum distribution from a federal fund. Additionally, consumers and retirees who are not wage earners are not eligible for this tax credit.

Inherited Funds / Lottery Winnings / Cash Consignment

In this phishing scheme, recipients receive an e-mail claiming to come from the U.S. Department of the Treasury notifying them that they will receive millions of dollars in recovered

funds or lottery winnings or cash consignment if they provide certain personal information, including phone numbers, via return e-mail. The e-mail may be just the first step in a multi-step scheme, in which the victim is later contacted by telephone or further e-mail and instructed to deposit taxes on the funds or winnings before they can receive any of it. Alternatively, they may be sent a phony check of the funds or winnings and told to deposit it but pay 10 percent in taxes or fees. Thinking that the check must have cleared the bank and is genuine, some people comply. However, the scammers, not the Treasury Department, will get the taxes or fees.

Form W-8BEN

In this scam, fraudsters modify a genuine IRS form, the W-8BEN, Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding, to request detailed personal and financial information. This could include nationality, passport number, bank account and PIN numbers, spouse's name and mother's maiden name, or other personal or financial information or security measures for financial accounts. The scammers may use the genuine form number and name or may make up a new form number, such as W-4100B2.

They either e-mail or fax the form or letter. If only a letter, the letter itself contains the request for the personal and financial information. The letter, which claims to come from the IRS, states that the recipient will face additional taxes unless he or she quickly faxes the required information to the number provided by the scammer.

In reality, taxpayers file the genuine Form W-8BEN with their financial institutions, not with the IRS. Additionally, the genuine W-8BEN does not request the taxpayer's passport number, bank account number, security or similar information.

Refund Scam

The bogus e-mail, which claims to come from the IRS, tells the recipient that he or she is eligible to receive a tax refund for a given amount. It instructs the recipient to click on a link contained in the e-mail to access and complete a form for the tax refund. The form requires the entry of personal and financial information. The refund scam is the most common one seen by the IRS. Several recent variations on this scam have claimed to come from the Exempt Organizations area of the IRS. Some others have included the name and purported signature of a genuine or a made-up IRS executive.

Taxpayers do not have to complete a special form to obtain a refund. Taxpayer refunds are based on the tax return they submit to the IRS.

How to Spot a Scam

Many e-mail scams are fairly sophisticated and hard to detect. However, there are signs to watch for, such as an e-mail that:

- Requests detailed or an unusual amount of personal and/or financial information, such as name, SSN, bank or credit card account numbers or security-related information, such as mother's maiden name, either in the e-mail itself or on another site to which a

link in the e-mail sends the recipient.

- Dangles bait to get the recipient to respond to the e-mail, such as mentioning a tax refund or offering to pay the recipient to participate in an IRS survey.

- Threatens a consequence for not responding to the e-mail, such as additional taxes or blocking access to the recipient's funds.

- Gets the Internal Revenue Service or other federal agency names wrong.

- Uses incorrect grammar or odd phrasing (many of the e-mail scams originate overseas and are written by non-native English speakers).

- Uses a really long address in any link contained in the e-mail message or one that does not start with the actual IRS Web site address (www.irs.gov). To see the actual link address, or url, move the mouse over the link included in the text of the e-mail.

What to Do

The IRS does not initiate taxpayer contact via unsolicited e-mail or ask for personal identifying or financial information via e-mail. If you receive a suspicious e-mail claiming to come from the IRS, take the following steps:

- Do not open any attachments to the e-mail, in case they contain malicious code that will infect your computer.

- Do not click on any links, for the same reason. Also, be aware that the links often connect to a phony IRS Web site that appears authentic and then prompts the victim for personal identifiers, bank or credit card account numbers or PINs. The phony Web sites appear legitimate because the appearance and much of the content are directly copied from an actual page on the IRS Web site and then modified by the scammers for their own purposes.

- Contact the IRS at 1-800-829-1040 to determine whether the IRS is trying to contact you.

- Forward the suspicious e-mail or url address to the IRS mailbox phishing@irs.gov, then delete the e-mail from your inbox.

Genuine IRS Web site

The only genuine IRS Web site is IRS.gov. All IRS.gov Web page addresses begin with http://www.irs.gov/. Anyone wishing to access the IRS Web site should initiate contact by typing the IRS.gov address into their Internet address window, rather than clicking on a link in an e-mail.